科 技 政 策 参 考

SCIENCE AND TECHNOLOGY POLICY COURIER

2016 年第 02 期（总第 89 期）

中国科学技术发展战略研究院

科技体制与管理研究所　主办　　2016 年 02 月 25 日

目　录

《民法总则》拟采用新的法人分类标准

党的十八届四中全会提出“编纂民法典”的重大任务。民法典在我国法律体系中的地位仅次于宪法，对完善社会主义市场经济体制、保障人民群众权利具有重大意义，是影响国计民生的根本大法。

由于我国未来的民法典将是一部涵盖合同法、物权法、侵权责任法、婚姻法、继承法等的综合性法条体系，其编纂也是一个长期的过程。当前，我国民法典的编纂工作主要集中在修订《民法通则》为新的《民法总则》上。

全国人大常委会法制工作委员会于2015年4月正式启动了民法典编纂工作，决定首先进行民法总则的起草。中国法学会民法典编纂项目领导小组组织撰写的《中华人民共和国民法典·民法总则专家建议稿（征求意见稿)》已初步完成，并向社会公开征求了意见。

征求意见稿第三章改变了我国现行《民法通则》中企业法人、机关法人、事业单位法人和社团法人的分类方法，改设机关法人、社团法人和财团法人，并进一步将社团法人分为营利性社团法人和非营利性社团法人。其中营利性社团人包括企业法人和农民专业合作社法人等；非营利性社团法人，包括事业单位法人和非基金会社会团体法人。

征求意见稿还设立了大陆法系国家普遍采用的财团法人，并规定财团法人是指利用自然人、法人或者其他组织捐助的财产，以从事慈善、社会福利、教育、科学研究、文化、医疗、宗教等特定公益事业为目的，依照法律规定成立的非营利性法人。财团法人包括基金会、民办非企业等形式。

新的法人分类方式，放弃了我国计划经济时期形成的《民法通则》按照企业、非企业划分法人类型的基本逻辑，首次在法人制度的整体结构方面体现了私法人和公法人的区分，营利法人和非营利法人的区分，社团法人和财团法人的区分。这是我国民事法律的重大变化。

考虑到我国已有大量民办公益性科研机构、地方产业技术研究院

等新型研发机构快速涌现，新的法人分类体系将对此类机构的发展产生重要影响，对此我们将给予持续关注。

（李研 撰写）

地方政府践行权力清单制度的历程及现状

《中共中央关于全面深化改革若干重大问题的决定》明确指出，要强化权力运行制约和监督体系，推行地方各级政府及其工作部门权力清单制度，依法公开权力运行流程。自此，权力清单概念逐渐被公众所熟知，并成为学界研究讨论的热点，各地政府也相继开展起权力清单制度的建设。

对“权力清单”概念最早的实践于 2005 年，始于河北省。2009 年，中纪委、中组部开展了县委权力公开透明运行试点工作。十八届三中全会后，中央对加强政府权力监督工作提出明确要求，并成立专门工作小组予以推动，各地政府权力清单制度的建设工作全面铺开。2014 年 5 月至 2015 年 12 月，广东、安徽、浙江、江苏等 19 个省（市）陆续公布了各自省级政府的权力清单，2016 年将基本实现各市县（区）级层面权力清单的全部公布。此外，继安徽省首次公布了该省省级政府的责任清单之后，当前各省份责任清单的编制工作也在逐步落实。

由于权力清单制度是一项新生事物，尚无固定的程式可循。通过对广东、安徽、江苏、北京等省市的调研发现，各方对权力清单的认识和实践比较一致，都是按照法定职权概念及职权类别进行分类，首先各部门按照所规范的统一梳理口径全面梳理现有的行政职权，晒出权力家底；其次，按照简政放权的要求，各部门对梳理出的行政职权逐项提出保留、下放、取消、调整的意见；再次，通过征求相关部门意见、专家论证、合法性审查、提请审议等进行审核确认；最后，公布运行，将职权名称、类别、编码、依据、实施主体和监督方式等基本信息予以公开，建立清单管理制度和动态运行机制。

目前各省（市）对责任清单的认识和做法还不统一：广东省认为权力和责任是一体两面，按照权力清单中“9+X”的分类编制了“权责清单”；江苏、浙江省认为部门“三定”就是法定职责，也是法定责任，并以此为基础细化出部门责任；安徽省认为权力行使过程中的应尽义务和应承担的不利后果是部门责任，对每一项行政职权都依据运行程序细化了责任事项和相应的追责情形；南京市的部门责任清单包括公共决策与行政指导类事项、行政权力（含行政许可）类事项、公共服务类事项、职责边界事项和内部管理类事项 5 个方面，把行政权力类事项作为部门责任清单的一部分；北京市采用的是“通用责任清单+专项责任清单”的模式，其中，通用责任清单对每类行政职权运行中各个环节的共性责任事项按照法定流程进行了梳理，专项责任清单的编制则试图立足北京市实际，围绕北京市中心工作和重点任务，厘清不同热点领域的责任分工和责任事项，首次制定的专项责任清单将着眼于“城市病”的治理，覆盖人口调控、环境保护、违建治理等 6 个领域。

资料来源：郑俊田、郜媛莹，中国行政管理，2016 年第 2 期。

（林娴岚 摘编）

美国大学与国家实验室关系中的三类专有性资产

大型高能加速器等“大科学装置”的出现是 20 世纪科学发展的一个重要特征。对于大科学装置，不同的地区或国家有着各异的管理模式。如欧洲核子研究中心的多国联合管理模式、德国的“亥姆霍兹学会”模式、日本的独立行政法人模式、以及美国国家实验室的“政府所有，政府管理”或“政府所有、合同管理”等模式。对于美国，又以“依托大学建立与管理国家实验室”模式最为著名（以下简称“美国模式”），它属于“政府所有、合同管理”的一种。

约从 2004 年起，“美国模式”受到国内学界的普遍关注，美国许

多世界一流大学的崛起被认为得益于此，如加州大学与伯克利劳伦斯国家实验室。“美国模式”的主要优势是实现大学和国家实验室的资源互补，例如，国家实验室可以通过提供先进的科研装置和条件，为学校整体学术水平的提升做出贡献；而大学则能够为国家实验室提供多学科的人才储备和学术支撑，拓展国家实验室解决关键科学问题的能力。在合作中，三类专有性资产的情况如下：

（1）专有性场地。国家实验室的选址取决于大科学装置，因为这类装置的位置一旦固定，再移动的成本将非常巨大。例如，美国斯坦福直线加速器中心所建造的直线加速器，占地 426 英亩，主加速器长达 3.2 公里，深埋于 10 米深的地下。然而，大部分美国国家实验室的选址并不“紧挨着”某所大学。在移交管理权之前，加州大学就曾是位于新墨西哥州的洛斯阿拉莫斯国家实验室的合同管理方。因此，美国的国家实验室与大学虽然彼此有着合作的需要，却也远远没有形成类似于煤矿工程与燃煤电厂那样紧密的原材料供求关系。

（2）专用性实物资产。作为美国国家实验室的关键物质基础，建造大科学装置所耗费的资源往往以“亿美元”计数，一个国家在某个特定的研究领域上通常只斥资建设一种大科学装置。这样的装置不可能专属于某个大学所有，它不仅产权属于国家，其目的也是为国家科技与社会经济发展服务，是一种国家战略性投资。企业投资某种专用性实物资产是为了获得市场竞争优势，而在开放共享的制度下，国家投资的大科学装置和国家实验室，每个大学及其它组织机构都有机会获得其中的服务和资源支持。因此，大科学装置虽然是有着特定用途的专用性实物资产，但这种资产并没有使得大学与国家实验室产生高度紧密的双边依赖关系，并不需要建立一体化治理结构。

（3）专用性人力资本。如果大学与国家实验室投入了能产生双边依赖的专用性人力资本，那么应当能观察到这两种组织有着大量且长期共聘的固定人员。实际并非如此。一方面，“共聘人员”是美国国家

实验室与其他研究机构的一种传统合作方式，并不固定于某所特定的大学。而且，美国国家实验室主要采用“基于项目（project-by-project）”的运作方式，因项目需要而组建研究队伍，研究人员可以来自全国、乃至世界的其他研究机构，这个队伍随着项目的结束而解散。另一方面。即使在依托美国大学管理运营的国家实验室中，共聘人员占总固定人员总数的比例并不大，例如劳伦斯伯克利国家实验室中的共聘人数占总人数的 7%，普林斯顿等离子体实验室的这个数字则是 2%。此外，在有别于企业的高度开放性制度下，美国国家实验室每年的流动科学家就占据了相当高的比例，如阿贡国家实验室 2012 年的访问科学家就占了总人数 30%左右，这为实验室的研究工作贡献了很大一部分的人力资本。

资料来源：黄振羽 丁云龙，科学学研究，2015 年第 6 期。

（李哲 摘编）

美《网络安全国家行动计划》旨在强化未来网络竞争优势

2016 年 2 月 9 日，奥巴马公布《网络安全国家行动计划》（CNAP），该计划意在从网络基础设施、专业人才、与企业合作等五个方面，全面提高美国在数字空间的安全。该行动计划提议在国会 2017 财政年度预算中专款（190 亿美元）资助，第一次设立联邦首席信息安全官（CISO），下令成立国家网络安全促进委员会、联邦政府隐私委员会等措施，值得关注。

一是目标是以网络安全控制占领网络发展的制高点。近二十年来，基于网络的新经济、创新者和企业促进美国经济增长，并使得美国在全球居于领先位置。但是网络带来的安全威胁日益成为制约网络应用与发展的核心问题，大有吞噬网络利益的势头。鉴于此，奥巴马政府发布了《网络安全国家行动计划》。它既提供了短期行动计划，也明示出了长期战略目标，包括提高对网络安全的关注和保护，保护隐私，

保证公众安全以及经济和国家安全，使美国民众能够更好地掌控数字安全，使企业能够安全地运营和保护信息，政府也能够保护民众及提交的信息。奥巴马表示，面对网络安全问题的复杂性和严峻性，需要采取一些大胆的行动，提升美国在全球数字经济中的竞争力。

二是措施兼顾短期与中长期。该计划既包含联邦政府近期行动，也有长期改进举措，如建立国家网络安全促进委员会、建立信息技术现代化基金并设立联邦首席信息安全官、加强在线账户的保护等，旨在全面提升联邦政府、私营企业以及个人生活的网络安全。该计划的以下两个要点值得关注：

第一通过“国家网络安全联盟联合主流企业与服务公司，发起新的国家网络安全宣传行动，专注多重认证，以提升、培育信息消费者的网络安全意识。该联盟为非营利性组织，其成员包括美国国土安全部（DHS）以及赛门铁克、思科、微软、SAIC 与 EMC 等私营企业。其呼吁并鼓励使用多重验证机制，同时实施一套尚未最终定名的“有效身份认证”方案。合作者包括 Google、Facebook、DropBox、Microsoft 等顶尖技术公司，以及 MasterCard、Visa、PayPal 和 Venmo 等交易服务公司。

第二，投资在网络空间安全人员培训教育上。（1）通过建立网络安全预备役（CyberCorps Reserve）计划，为想获得网络安全教育，并在民事联邦政府服务的美国人提供奖学金；（2）开设网络安全的核心课程，以确保想就职联邦政府的网络安全的毕业生，有必要的知识和技能；（3）加强《国家网络空间安全学术卓越中心计划》（National Centersfor Academic Excellence in Cybersecurity Program），以增加参与的学术机构和学生数量，通过程序和课程的演变，丰富学生的知识；（4）增加国家网络安全学术卓越中心项目内所涵盖的大学与高校数量，同时将奖学金数额同联邦政府网络安全核心课程与网络安全水平挂钩。

第三，加强消费者数据的安全性。（1）在加强多重身份验证和身份证明的同时，评估可以减少将社会安全号码作为公民身份标识符的使用频率的程序；（2）小企业管理局（SBA）与联邦贸易委员会、美国国家标准和技术研究所（NIS）、能源部将通过 68 个 SBA 小企业管理局区域办公室、9 个国家标准和技术研究所 NIST 制造业扩展合作中心和全国其他区域网络，为 140 万个小企业和小企业利益相关者提供网络安全培训。

第四，增强关键基础设施安全性和恢复能力。美国的国家和经济安全取决于国家关键基础设施的可靠运行。关键基础设施的业主与运营商的持续合作将提高网络和国家安全。

第五，带领国际社会，将这些准则变为负责任国家的行为准则。2015 年，G20 成员国与美国就重要规范达成一致，包括国际法在网络空间的适用性，各国政府不应该支持出于商业目的利用网络盗取知识产权的行为，欢迎联合国政府专家组发布相关报告、加强国际合作，防止对民用基础设施的攻击，支持计算应急小组提供重建和容灾服务。美国政府试图通过进一步的双边或多边承诺，建立信任措施，并实施这些准则。

（张赤东 摘编）

联系人：朱丽楠　　联系电话：010-58884632